Executive Summary

Overview

Systems Integration & Development, Inc. (SID) is pleased to submit an analysis report for the NOAA Office of Finance and Administration (OFA) Network System. The report covers the network infrastructure analysis, potential shortcomings of the network, potential solutions to eliminate any shortcomings and discusses the potential overall architectures.

The report has been constructed to "mirror" the discussion with various NOAA OFA Network System support staff. The purpose of this report is to analyze and evaluate the information provided. This report will present the current architecture and provide suggestions to improve the network performance further to reduce the Total Cost of Ownership (TCO).

Current Environment

The NOAA OFA Network System is a distributed network environment consisting of 4 campuses – HCHB, Gaithersburg, Germantown, and SSMC. The four campuses are connected through a commercial MAN service with 10 Mbps data throughput. The network operates on a Windows NT 4.0 environment. There are about 1000 users connected to the system for various services such as file, print, license, Internet, Calendar, and Messaging. The messaging service is supported by two Netscape Messaging Servers using IMAP protocol. The network supports Corel Office Suite for office automation products.

Current System Analysis

The NOAA network structure is based on the Single Domain Model. Because all user accounts and resources are within the same domain, there is no need to set up trust relationships. All the administrative tasks are handled by one central location.

SID analyzed a network traffic report (see Appendix A) generated by Concord Network Health – LAN/WAN. The data provided in this report depicted two main factors:

- There is enough network bandwidth available for future growth. A peak bandwidth utilization of $\leq$ 1%

of the 100 Mbps Fast Ethernet data rate.

- The OFA network system is presently being under-utilized and its capacity is sufficient to support the 1000 user environment.

There was a consensus among SID engineers and NOAA Network Systems Support staff that network monitoring tool may not be collecting all the traffic. The analysis indicated that in order to correctly evaluate the traffic pattern of the network, we should fine tune network monitoring tool. This will help in collecting additional traffic data for complete traffic pattern evaluation and for complete analysis of network capacity.

SID interviewed several NOAA network personnel and identified the following problem areas regarding system performance and inconsistencies:

- Inconsistent Disaster Recovery & Backup
- Inconsistent User Login process
- Inconsistent Printing process
- Inconsistent Licensing
- Inconsistent Web-based Applications
- Slow Messaging (E-Mail)

Areas For Improvement

SID Systems Engineers together with NOAA support personnel identified the following areas that need improvement:

- Disaster Recovery and Backup
- User Login
- Printing
- Messaging
- Licensing
- Web-Based Applications
- Network and Web Security
- Software Distribution
- IP Addressing
- Network Monitoring
- Software Metering

Recommendations

Based on the information collected, SID performed detailed system analysis and suggests the following corrective actions :

1. Perform Detailed Network Traffic Analysis
2. Conduct Network Performance Tuning and Optimization
3. Improve and standardize Backup and Restore
4. Improve Disaster Recovery capability
5. Add Remote Monitoring and Remote Control Capability
6. Implement Proactive Technology Refresh
7. Automate Software Distribution process
8. Evaluate and design Web Architecture
9. Ensure greater Security

SID has specified the benefits and costs associated with each recommendation. These recommendations are mutually exclusive.

Risk Mitigation

There are no significant risks in implementing any of the recommendations. In addition, the recommendations will alleviate the following potential risks to the network:

- Bottlenecks
- Single point of failure in the network
- Faulty wiring in the network
- Viruses
- Intrusion
- Information privacy
- Complete shutdown

Summary

The improvements to the NOAA network are classified in three areas:

- System inconsistencies
- System performance
- System enhancements

Firstly, SID recommends that NOAA should reduce inconsistencies from their network. Secondly, SID recommends that NOAA should improve the network performance. Finally, SID recommends that NOAA should implement enhancements to their network to reduce the TCO.

By improving and fine tuning the network, NOAA can achieve the following benefits:

- Increased productivity
- Increased security
- Better sharing of resources
- Better user satisfaction
- Reduced TCO
- Increase network capabilities easily

1 Current System Description

The NOAA OFA Network System is a distributed network environment consisting of 4 campuses – HCHB, Gaithersburg, Germantown, and SSMC. The four campuses are connected through a commercial MAN service with 10 Mbps data throughput. The network is operated in the Windows NT environment and it is structured in a Single Domain architecture with the Primary Domain Controller (PDC) located in SSMC and one Backup Domain Controller (BDC) per site in the other three campuses. There are about 1000 users connected to the system for various services such as file and print, license, Internet, Calendar, and messaging. The messaging service is supported by 2 Netscape Messaging Servers using IMAP protocol.

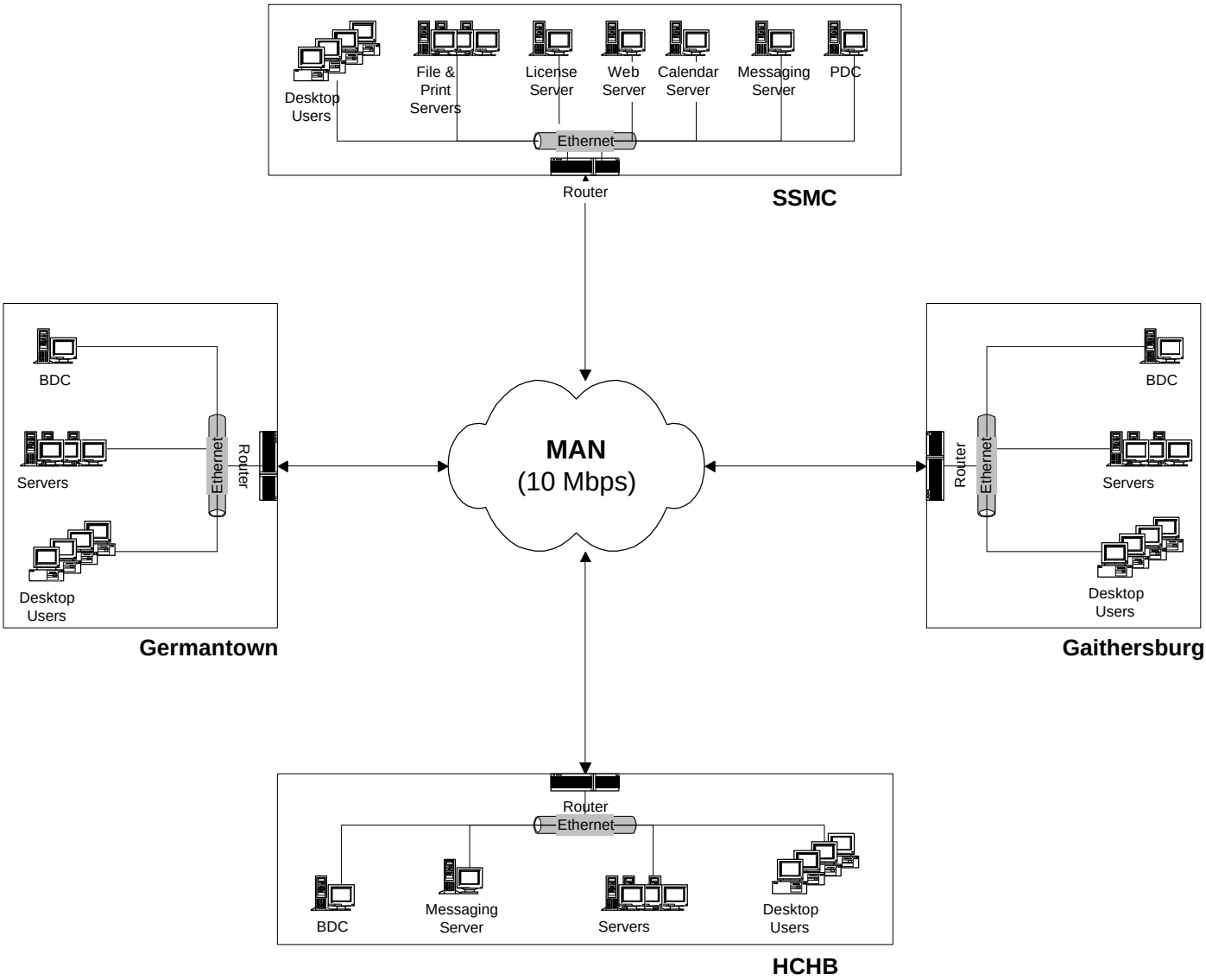


Figure 1 NOAA OFA Network System

2 Current System Analysis

An analysis on the current NOAA Network System based on interviewing NOAA personnel (see Appendix C for Interview Summary) showed the following characteristics regarding network traffic, performance, operations, and network architecture:

2.1 User Administration

The NOAA network structure is based on the Single Domain Model. Since all user accounts and all resources are within the same domain, there is no need to set up trust relationships, and all the administrative tasks are handled in one central location at SSMC. This is the Microsoft's preferred model for networks with fewer than 15,000 users. For organizations similar to NOAA that have different departments that need to administer their own resources, one might want to consider other domain models such as Master Domain Model, Multiple Master Domain Model, or the Complete Trust Domain Model. See Section 4 for further details regarding various alternatives.

2.2 Network Traffic

A network traffic report (see Appendix A) generated by Concord *Network Health–LAN/WAN* was presented to and analyzed by SID. This report recorded network traffic passing through the OFA SSB Cisco Router between 3/3/99 and 3/15/99, and it showed a peak bandwidth utilization of 0.88 Mbps (≤ 1% of the 100 Mbps Fast Ethernet data rate). The analysis indicated that the OFA network system is actually under-utilized and its capacity is sufficient to support the 1000 user environment. There was a consensus among SID engineers and NOAA Network System Support staff that network monitoring tool may not be collecting all the traffic. The analysis indicated that in order to correctly evaluate the network traffic pattern, we should fine tune network monitoring tool to collect additional data. This will enable complete analysis of traffic data and will help in establishing a baseline for network capacity.

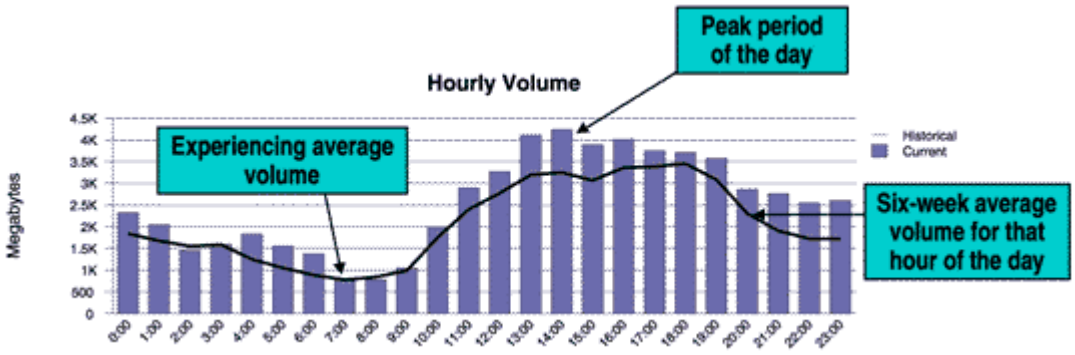


Figure 2. Sample Data as per Concord Network Health-LAN/WAN report

2.3 System Performance/Consistency

SID prepared a questionnaire (See Appendix-B) to guide through the interviewing process. After interviewing several NOAA network personnel and analyzing the present environment, SID had identified some problem areas regarding system performance and inconsistency:

Problem Area	Problem Type	Problem Description
Disaster Recovery & Backup	Inconsistency	No established processes and procedures to do disaster recovery
User Login	Inconsistency	Occasional user login failures
Printing	Inconsistency	Printer drops off when starting one particular File/Printer Server
Licensing	Inconsistency	Occasional errors in granting application license
Web-based Applications	Inconsistency	Potential problems in managing web-based applications
Messaging	Performance	Slow e-mail service

A detailed discussion on these problem areas will be presented in Section 3

2.4 Network Operation and Maintenance

Operation and Maintenance of the NOAA network are mostly done in a manual fashion. Static IP addresses are used throughout the whole network instead of adopting the Dynamic Host Configuration Protocol (DHCP) for dynamic IP acquisition. Automatic software distribution is not available; therefore, all the software updates have to be manually installed by the system administrators, which may not be cost effective or efficient.

2.5 Network Architecture

Several key components (e.g., Netscape Messaging Server) of the NOAA network do not have back-up units available and therefore could be classified as Single Point of Failure in the system. Potentially costly system failure and subsequent severe downtime may be possible.

2.6 Network Performance Monitoring

Network monitoring activities were not observed during the interview period even though software-monitoring tools such as HP OpenView and Cisco Works were available at NOAA for that purpose.

3 Areas for Improvements

This section addresses some current or potential problem areas identified by either NOAA personnel or SID Systems Engineers during the System Interview Process. Table 1 lists all these problem areas along with their possible causes, and suggestions for solving or improving these problem area performances.

Table 1. Areas for Improvements

Problem Area	Description	Possible Causes	Suggestion
Disaster Recovery and Backup	• Troublesome performance	• Improper backup tools	• Perform trade-off analysis to come up with backup tools suitable to the system
User Login	• Occasional user login failures (no domain controller available))	• Time-out for User Login request due to network traffic congestion • Improper performance tuning	• Analyze network traffic with network traffic analysis tools (e.g., Microsoft Network Monitor). Optimize network performance by fine-tuning the system based on traffic analysis results.
Printing	• Printer drops off when starting one particular File/Printer Server	• Printer configuration conflict	• Analyze event log to trace the problem • Add dedicated print server to the system
Messaging	• Slow e-mail service	• Inadequate hardware equipment • Improper performance tuning	• Perform load analysis to decide hardware competency • Analyze message traffic with network traffic analysis tools (e.g., Microsoft Network Monitor). Optimize messaging performance by fine-tuning the system based on traffic analysis results.
Licensing	• Occasional errors in granting application license	• Time-out for License request due to network traffic congestion	• Analyze network traffic with network traffic analysis tools (e.g., Microsoft Network Monitor). Optimize network performance by fine-tuning the system based on traffic analysis results.

Problem Area	Description	Possible Causes	Suggestion
Web-Based Applications	• Potential problems in managing web-based applications	• No standards utilized in implementing web-based applications	• Evaluate and design the architecture for web-based applications
Network & Web Security	• The system is vulnerable to external intrusion	• Lacking network security features • Lacking web security features	• Adding fire-walls to current system (underway) • Establish web security
Software Distribution	• Software distribution and updating is time consuming	• Manual distribution of software packages	• Adding automatic software distribution capability (e.g., Novadigm EDM)
IP Addressing	• Reassigning IP address will require significant human resource and cause network services delay	• Static IP address assignment	• Adding DHCP service to the network
Network Monitoring	• The system is vulnerable to human errors and problem tracking and fixing is time consuming	• Network performance and health are not monitored in real-time	• Implement automatic network monitoring capability by adapting network monitoring tools such as HP OpenView and Cisco Works
Software Metering	• Desktop computers have various kinds of software installed. No control on licensing issues	• Lacking software licensing control	• Implement software metering capability to monitor and control software licensing

3.1 Backup and Storage Management

NOAA's success is tightly coupled with its ability to store and manage information. With the amount of data growing at an incredible rate, SID can help NOAA implement a storage strategy that will keep pace. Traditional backup utilities, designed for the needs of small PC LAN environments, are no longer adequate to meet the complex storage protection requirements for rapidly growing distributed networks.

A modern day storage system similar to NOAA's must:

- Be cost-effective
- Prevent data loss
- Offer adequate, easily scaleable storage
- Provide fast access to data without interruptions
- Be able to deal with hardware failures

A strategy designed to address these issues consists of three inter-related components:

Data Backup: Data backup is a process that stores redundant copies of files from hard disk to removable media (usually tapes). The redundant copies of files are used or "recovered" in case the original file are damaged or accidentally deleted. Backup is ordinarily scheduled to run on a daily basis.

Data Archiving: Data archiving is the process of taking a "snapshot" of a file or a series of related files as it resides on primary media (disk) at a given point in time. The image of the snapshot typically resides on removable media – usually tapes or optical disk. Once the snapshot is "safely" stored on removable media, the necessary files can optionally be deleted from the primary storage. Unlike data backup, the act of initiating data archiving is controlled by the end user. Unlike data backup, it is not practical or wise to have a "network-wide one size fits all" archiving policy. End users define specific archiving policies that match their application needs.

HSM: Hierarchical Storage Management is a policy driven data management strategy where data is moved or automatically migrated from one storage medium to another based on a set of policies. After a file has been migrated from primary storage to secondary storage, it can later be staged to tertiary storage based on a set of policies.

The goals and characteristics of backup, archiving and HSM can be summed up as follows:

- The goal of backup is to protect data against accidental loss or damage. Backups should be reliable and efficient.
- The goal of data archiving is to conserve on-line storage space. Reliability, safety and storage to inexpensive media are the primary characteristics.
- The goal of HSM is to decrease the overall cost of storage. Migration and caching of files should be automatic and reliable.

3.2 Disaster Recovery

Provide disaster recovery support to NOAA so that there is not a single point of failure in the network. The disaster recovery plan does not suggest a fault-tolerant system. It only suggests that in case there is a disaster, the network can recover from that disaster easily. Implement a disaster recovery plan so that the complete network is fully operational with minimum downtime. Identify network resources that are suspected to be linked to single point of failure, provide a solution to remove single point of failure contingency, and implement the selected solution. Define standard operating instructions (SOIs) that can be followed during the actual disaster recovery and/or disaster recovery drill.

The disaster recovery plan will provide the following benefits:

- Handle single failure of any resource easily
- Improve productivity
- Improve reliability of the network resources
- Improve consistency
- Establish management confidence in the network system

3.3 Network Traffic Analysis

In order to identify performance problems and bottlenecks, we have to perform a detailed network traffic analysis. Microsoft Network Monitor is recommended for such analysis since it can perform detailed packet-by-packet analysis by decoding MSRPC packets. These packets are used in several types of network traffic (replication, e-mail, etc.) and if you can't decode them they are shown as TCP packets, which makes it almost impossible to understand what higher level protocol is being used. Network monitoring tools such as HP OpenView or Cisco Works will be used to detect network events and to collect performance data.

3.3.1 Network Traffic Optimization

The network traffic can be optimized once a network traffic analysis is done. Network traffic can be optimized in several areas:

- Client Initialization Traffic
  - DHCP
  - WINS
  - File Session
  - Logon Validation
- Client-to-Server Traffic
  - Browser
  - Domain Name System
  - Web-based browsing
- Server-to-Server Traffic
  - Account Synchronization
  - Trust Relationships

- Server Browser Traffic
- WINS Replication
- Directory Replication
- DNS Server

3.4 Web-Based Applications

Provide system architecture support to implement client/server software development infrastructure at the NOAA. Produce a complete framework for client/server software development environment. Define acceptance criteria for client/server software applications development so that they are easier to manage and maintain. Define enterprise application development infrastructure to include CORBA, HTML, Java, Oracle and DCOM.

This infrastructure will provide following benefits:

- Enable NOAA to develop web application easily and efficiently
- Improve productivity
- Improve incremental engineering of web applications
- Improve consistency among applications
- Maintain seamless environment among applications

3.5 Security

The security is most important criteria that are puzzling all the organization in a network environment. With the increased use of web, it has become very important component of any organization. NOAA is not an exception. The security is a very simple concept. There are only three components:

1. The client
2. The server
3. The connection between the two

The client requests resources from the server. The server provides resources to the client. It is a very simple concept and it is based on many assumptions. What can go wrong?

From the users point of view

- The server provides security for my information
- The documents I receive are free from dangerous viruses and malicious intent
- The server does not provide access to my information to people who are not supposed to have that information

From the server point of view

- The user will not be able to break into the server or alter the content of the server
- The user will not try to gain access to documents that he/she is not privy to
- The user will not crash the system and make it unavailable to other users

- If the user has identified himself, he is who he claims to be

From connection point of view

- The network connection is free from third-party eavesdroppers listening in on the communication line.
- The information sent between client and server is delivered intact, free from tampering by third parties.

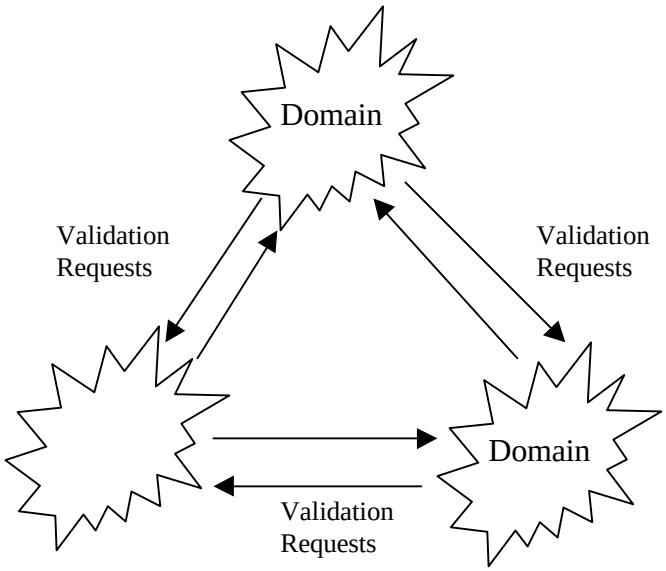
Implement NOAA policy to protect client, server, connection, and information resources. The security will provide following benefits:

- Enable NOAA to protect privacy and confidentiality of the information
- Avoid risks to the agency
- Provide client-side security
- Provide anti-virus capabilities so that all the information is virus-free
- Provide connection security so that the information never goes into unwanted hands
- Eliminate any chances of evesdropping

4 Alternatives

4.1 Multiple Domains with Trust Relationship

Administrative Autonomy on campus level is a major concern on the current Single Domain environment. The network resources are centrally controlled by the PDC at SSMC and system administrators on each campus have no direct control over their campus resources without going through PDC first. One alternative to this concern is to establish a separate domain for each campus and then set up multiple trust relationships between domains to get access to any resource in any domain. Figure 3 shows multiple trust relationships in which each domain has its own administration and controls for granting access to its users and it also grants access rights to other domains.



There are advantages and disadvantages related to this multiple trust relationships approach:

:

- Campuses control their networks and only allow other campuses to access their resources as needed

:

- Increase server-to-server traffic between domain controllers
- Extra network traffic between domain controllers for access granting

4.2 Single Domain with Remote Control Capability

Another alternative to give campus administrators some control over their campus resources is to provide remote control capability for the system. Campus administrators would be given authority to access PDC remotely using remote control tools such as Remote Desktop or PC Anywhere to control their own resources. The advantages and disadvantages associated with this approach are:

Advantages:

- Local administrators have limited control over their own network from their local site

Disadvantages:

- Extra processing requirement on PDC
- Only one remote session is allowed at any time

5 Risk Mitigation

There is no significant risk in implementing any of the recommendations. In addition, the recommendations will alleviate the following potential risks to the network:

- Bottlenecks
- Single point of failure in the network
- Faulty wiring in the network
- Viruses
- Intrusions
- Information privacy
- Complete shutdown

6 Recommendations

The following table lists recommendations NOAA can take to improve their network performance and health, cost range related to each recommendation, and how NOAA can benefit from these recommended actions:

Recommendation	Cost	Benefits
1. Perform Detailed Network Traffic Analysis	Low	• Get a better understanding of the current network performance under various circumstances • Identify performance bottlenecks • Identify causes for performance degradation
2. Conduct Network Performance Tuning and Optimization	Low	• Improve network performance by fine-tuning system parameters • Eliminate performance bottlenecks • Optimize system performance based on current load analysis and future load projection
3. Improve and standardize Backup and Restore	Medium	• The goal of backup is to protect data against accidental loss or damage. Backups should be reliable and efficient. • Reliability, safety and storage to inexpensive media are the primary characteristics. • The goal of HSM is to decrease the overall cost of storage. Migration and de-migration should be automatic and reliable.
4. Improve Disaster Recovery capability	Medium	• Handle single failure of any resource easily • Improve productivity • Improve reliability of the network resources • Improve consistency • Establish management confidence in the network system
5. Adding Remote Monitoring and Remote Control Capability	Medium	• Able to track system status in real-time • Able to provide filtered information by correlating network events • Facilitate system administration with remote control capability • Reduce overall human effort in managing the network • Reduce downtime with real-time detailed system status information

Recommendation	Cost	Benefits
6. Implement Proactive Technology Refresh	Low	• Actively monitoring system service status by establishing a hardware/software component database • Advance warning for system administrator when hardware reaches its Mean Time Between Failure (MTBF) • Advance warning for system administrator when software utilization reaches a predefined threshold of its capacity
7. Automated Software Distribution	Medium	• Cost effective, reliable system for the automated deployment and management of advocated software packages (including operating systems) within the enterprise for Windows and UNIX platforms • Manage NOAA applications easily and efficiently • Improve productivity • Maintain consistency among application configuration • Help maintain virus database consistently
8. Web Architecture	Low	• Enable NOAA to develop web application easily and efficiently • Improve productivity • Improve incremental engineering of web applications • Improve consistency among applications • Maintain seamless environment among applications
9. Security	Low to Medium	• Enable NOAA to protect privacy and confidentiality of the information • Avoid risks to the agency • Provide client-side security • Provide anti-virus capabilities so that all the information is virus-free • Provide connection security so that the information never goes into unwanted hands • Eliminate any chances of eavesdropping

Summary

The improvements to the NOAA network are classified in three areas:

- System inconsistencies,
- System performance, and
- System enhancements.

Firstly, SID recommends that NOAA should remove system inconsistencies from their network. Secondly, SID recommends that NOAA should improve the system performance. Finally, SID recommends that NOAA should implement enhancement to their network. By implementing this phased approach for improving and fine tuning the network, NOAA can achieve the following benefits:

- Increased productivity
- Increased security
- Better sharing of resources
- Better user satisfaction
- Reduced TCO
- Increase network capabilities easily

APPENDIX – B

NOAA SAMPLE QUESTIONNAIRE

High Level Areas/Questions to be covered during Information Gathering and Needs Analysis Phase:

I **Network infrastructure**

- How many servers are installed?
- How are those servers configured?
- How many users are they supporting?
- What type of users – what are the applications currently running and which ones are needed to be added on the desk tops?
- What types of Operating Systems are being used on the desk tops?
- What is your current network capacity?
- User specific requirements?

II **Performance related questions**

- Are you satisfied with the network performance?
  Yes …… No …….
  Reasons ……..
  ……

- Are you able to access / use/ transfer the following conveniently -
  1. Data files Yes ……. No ……..
  2. Messages Yes ……. No ……..
  3. Softwares Yes ……. No ……..
  4. Other resources (Specify) ……

- What is the delay time in accessing / using/ transferring the following -
  1. Data files ……..
  2. Messages ……..
  3. Softwares ……..
  4. Other resources (Specify) ……

- Are you satisfied with the following features of the present network –
  1. Speed Yes ……. No ……..
  2. Accuracy Yes ……. No ……..
  3. Accessibility Yes ……. No ……..
  4. Confidentiality Yes ……. No ……..

III Network Traffic Measurement

- How much load do you have on the network?
- What is the average size of files that are transferred?
- What is the maximum size of files transferred on the traffic?
- How many files are transferred per hour or in peak network usage time?
- How are printers set up and configured?
- Do your various sites need to maintain independent structure along with some need for exchanging traffic with the host server? List details regarding network entity relationship.
- How much traffic do you have on the Internet?
- How much traffic do you have on the e-mail?
- Do you use video / audio conferencing facilities on your network? If yes, to what extent?
- Do you use collaborator software anywhere?
- Do you have Roaming profiles?
- What happens to the Home directory when people roam from site to site? Does it remain the same?
- Who does database access?
- What tools are used to access the database?

Note :- Regarding measuring network traffic and/or load, there are many SNMP (Simple Network Management Protocol) based tools available in the industry. SID has used IBM NetView, HP Openview, Seagate NerveCenter, Fore Systems ForeView and many other SNMP compliant tools for system monitoring and management. SID will use any SNMP compliant tool that NOAA has and it is currently using in their enterprise. In case, NOAA does not have SNMP tool, SID will not require NOAA to purchase the tool for the requirement analysis. The simple network load information can be collected using other traditional methods. Alternatively, SID may decide to use some SNMP based tool to estimate the network traffic without the need for NOAA to purchase that tool. There are many ways to estimate the traffic. SID has successfully done this kind of work for many large corporations including Lockheed Martin, Raytheon, MCI and GTE.

IV Problem variance / Suggested improvements

- What kinds of system improvement are desired by management, users and system administrators? Are their any suggested areas of focus for improvement?
- Areas of current bottlenecks?

V Growth potential

- What kind of growth do you anticipate in terms of network traffic, number of users, additional sites, etc.?

VI **Network Security**

- What kind of security issues/ concerns must be addressed?
- What kind of Firewall set up do you have?

NOTE: This is a broad list of questions. As we talk to the users and system administrators, we will augment this list to improve the network infrastructure.

APPENDIX – C

Questionnaire		Responses			Areas for Improvement	Recommendation
		#1	#2	#3		
I	**Network infrastructure**					
	How many servers are installed?	11	N/A	N/A		
	How are those servers configured?	Single Domain	Single Domain	Single Domain	Remote systems administrators can not manage their resources	Adding Remote Monitoring and Remote Control Capability
	How many users are they supporting?	270/SS, ~600 whole OFA network	1000 users (5 sites)	750 users		
	What type of users – what are the applications currently running and which ones are needed to be added on the desk tops?	Non-scientific users, Mostly database and desktop applications	Standard desktop users, WordPerfect/Corel 8 Suite	N/A		
	What types of Operating Systems are being used on the desk tops?	Windows 95, Windows NT	Windows 95, some Windows NT	Windows 95, Windows NT		
	What is your current network capacity?	N/A	Designed for 10,000 users	N/A		Perform Detailed Network Traffic Analysis
	User specific requirements?	N/A	N/A	N/A		
II	**Performance related questions**					
	Are you satisfied with the network performance?	Not too satisfied, problem with user login and print service	Yes	Mail is slow , 10-15 sec time delay in accessing Inbox	1. User Login 2. Messaging	Perform Detailed Network Traffic Analysis
	Are you able to access / use/ transfer the following conveniently					
	1. Data files	yes	yes	yes		Perform Detailed Network Traffic Analysis
	2. Messages	yes	No, getting message is slow	no	Messaging	Conduct Network Performance Tuning

					and Optimization
3. Softwares	Desktop computers have various kinds of software installed. No control on licensing issues	Occasional errors in granting application license	N/A	1. Licensing 2. Software Distribution 3. Software Metering	Automated Software Distribution
4. Other resources (Specific)	N/A	N/A	N/A		
What is the delay time in accessing / using/ transferring the following -					
1. Data files	No significant delay	No significant delay	No significant delay		Perform Detailed Network Traffic Analysis
2. Messages	No significant delay	Some delay	Some delay	Messaging	Conduct Network Performance Tuning and Optimization
3. Softwares	No significant delay	N/A	N/A		
4. Other resources (Specify)	N/A	N/A	N/A		
Are you satisfied with the following features of the present network –					
1. Speed	yes	yes	yes		Perform Detailed Network Traffic Analysis
2. Accuracy	yes	yes	yes		Perform Detailed Network Traffic Analysis
3. Accessibility	yes	yes	yes		Perform Detailed Network Traffic Analysis
4. Confidentiality	yes	yes	yes		Perform Detailed Network Traffic Analysis
III Network Traffic Measurement					

	How much load do you have on the network?	N/A	N/A	N/A		Perform Detailed Network Traffic Analysis
	What is the average size of files that are transferred?	N/A	N/A	N/A		Perform Detailed Network Traffic Analysis
	What is the maximum size of files transferred on the traffic?	N/A	N/A	N/A		Perform Detailed Network Traffic Analysis
	How many files are transferred per hour or in peak network usage time?	N/A	N/A	N/A		Perform Detailed Network Traffic Analysis
	How are printers set up and configured?	Printers are served by the file servers and there is problem when file server is rebooted	Print server for 95 workstations and HP Printer	N/A	Printing	Conduct Network Performance Tuning and Optimization
	Do your various sites need to maintain independent structure along with some need for exchanging traffic with the host server?	N/A	Sites are self-contained/ self-sufficient	N/A	IP Addressing	Adding Remote Monitoring and Remote Control Capability
	How much traffic do you have on the Internet?	N/A	N/A	N/A		Perform Detailed Network Traffic Analysis
	How much traffic do you have on the e-mail?	2 message servers maintaining 500 mailboxes for Gaithersburg and Germantown	No spam, files are attached in the mail to exchange information	2 Netscape messaging servers for 750 users	Messaging	Perform Detailed Network Traffic Analysis
	Do you use video / audio conferencing facilities on your network? If yes, to what extent?	no	no	no		
	Do you use collaborator software anywhere?	no	no	no		Automated Software Distribution
	Do you have Roaming profiles?	no	no	no		
	What happens to the Home directory when	no	Default working	no		

	people roam from site to site? Does it remain the same?		directory is part of server file system			
	Who does database access?	N/A	Oracle (no maintenance provided)	N/A		
	What tools are used to access the database?	Procomp, Syberprise	Oracle and SQL tools	N/A		
IV	**Problem variance/Suggested improvements**					
	What kinds of system improvement are desired by management, users and system administrators? Are their any suggested areas of focus for improvement?	1. Backup and disaster recovery 2. User login 3. Printer service	1. Upgrade our servers periodically 2. Proactive technology refresh 3. Troubleshooting capabilities 4. Test lab capabilities 5. Need to monitor traffic	1. Better hardware for messaging servers 2. Single approach for web-based applications 3. Network security	1. Disaster Recovery and Backup 2. User Login 3. Printing 4. Messaging 5. Web-Based Applications 6. Network & Web Security 7. Network Monitoring	1. Conduct Network Performance Tuning and Optimization 2. Improve and Standardize Backup and Restore 3. Improve Disaster Recovery Capability 4. Adding Remote Monitoring and Remote Control Capability 5. Implement Proactive Technology Refresh 6. Web Architecture 7. Security
	Areas of current bottlenecks?	1. Backup and disaster recovery 2. User login 3. Printer service	1. Processor may be bottlenecked (currently 166 MHz Pentium) 2. Workstations need more memory	1. Backup 2. No single point of entry for security 3. Outside user access cause system	1. Disaster Recovery & Backup 2. User Login 3. Printing 4. Mesaging 5. Network &	1. Conduct Network Performance Tuning and Optimization 2. Improve and Standardize Backup and

			3. Mail is slow	saturation	Web Security	Restore 3. Improve Disaster Recovery Capability 4. Adding Remote Monitoring and Remote Control Capability 5. Web Architecture 6. Security
V	**Growth potential**					
	What kind of growth do you anticipate in terms of network traffic, number of users, additional sites, etc.?	No significant growth is expected	1. more IP traffic 2. another 200 users 3. fold regional sites to this network	No significant growth is expected		
VI	**Network Security**					
	What kind of security issues/ concerns must be addressed?	N/A	virus	N/A		Security
	What kind of Firewall set up do you have?	Firewall in currently under development	No firewall setup currently	No firewall	Network & Web Security	Security